HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/468,157	12/21/1999	JAMES H. MOORE	D/99748	3291

7590 05/19/2005

John S. Zanghi Esq.
Fay, Sharpe, Fagan, Minnich & McKee LLP
1100 Superior Avenue
Seventh Floor
Cleveland, OH 44114-2579

EXAMINER	
SHIN, KYUNG H	

ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 05/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/468,157	MOORE, JAMES H.	
	Examiner	Art Unit	
	Kyung H. Shin	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 February 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. In view of the Appeal Brief filed on 2/14/2005, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

2. **Claims 1 - 7** are pending on this application. **Claims 1, 6, 7** are amended. Independent claim is **1**.

Response to Arguments

3. In reply to an obviousness rejection under 35 U.S.C. § 103, applicant argues that the secondary reference and primary reference combination is not allowed due to nonobviousness.

3.1 The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). Furthermore, in response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

3.2 In response to Applicant's arguments, 37 CFR § 1.111(c) requires applicant to "clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made".

Claim Rejections - 35 USC § 103

4. Claims 1, 4, 5, 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber et al. (U.S. Patent No. 5,136,647) in view of Romney et al. (U.S. Patent No. 6,085,322) and further in view of Berson et al. (U.S. Patent No. 5,949,879).

Regarding claim 1 (Previously Presented), a method for securing the integrity of files

prior to archiving of said files, involving an exchange between a client and a Time Source Provider said method comprising the steps of:

Haber discloses secure time-stamping of digital documents (see Haber col. 2, lines 33-36) between an agency (i.e. an organizationally associated third party, time source provider) and client, and verify by digital signatures. (see Haber col. 2, line 66 - col. 3, line 1: TSA, time stamp agency (i.e. organizationally associated entity))

e) Haber discloses a client (i.e. author) converts the digital document to a reduced digital size (see Haber col. 3, line 811) using oneway hash (see Haber col. 3, line 13: digital signature (i.e. hash)) to meet the step of transmitting encrypted data);

g) Haber discloses a TSA (i.e. Time Source Provider) creating a TimeMap as a time stamp receipt (see Haber Fig. 2, step 25) containing a current time (see Haber col. 4, line 1014), an ID of author, a hash of document, and receipt of the data, etc for each document (see Haber col. 4, line 8: data collection) with a variety of parameters as a string (see Haber col. 6, line 24), and cryptographic signatures. (see Haber col. 6, line 2830: utilized signature techniques);

h) Haber discloses TSA (i.e. time source provider) returns client's data along with certified (i.e. digital signature), TimeMap and encryption key signatures. (see Haber col. 4, line 23; col. 7, line 2);

i) Haber discloses TSA (i.e. time source provider) providing encrypted data back to the client (i.e. author). (see Haber step 27; col. 6, line 57; col. 6, line 68);

a) Romney discloses a client generating a key pair (see Romney Figure 2; col. 6, line 62-63);

c) and used for a cryptographic signature. (see Romney col. 7, lines 51-52) and attached to the document (see Romney col. 7, line 60);

d) encrypting client's files and message digest (see Romney col. 8, line 42);

b) Berson discloses generating an organizationally associated (i.e. certificate attached) a key pair; (see Berson col. 4, lines 29-34: public/private key generated with an associated certificate of authenticity)

f) decrypting encrypted data and file attributes with private key and then with the client's public key. (see Berson col. 4, lines 4-12: standard public/private key cryptographic techniques utilized, one key (i.e. public or private) is used to encrypt data, the other key is used to decrypt encrypted data)

It would have been obvious to one of the ordinary skilled in the art at the time the invention was made to modify Haber to generate TSA type cryptographic (public/private) key pairs utilized in data encryption/decryption techniques as taught by Berson, and to generate client public/private key pairs, sign encrypted data as taught in Romney. (see Romney col. 6, lines 62-63) One of ordinary skill in the art would be motivated to employ Berson in order to optimize and enhance procedures in the generation and authentication of digital signatures. (see Berson col. 2, line 12-13: " ... *provides for a audit-able, secure environment for the generation of cryptographically protected digital data* ... "),

and to employ Romney in order to enhance and optimize effective security in encryption key generation and processing. (see Romney col. 4, lines 32-37: " ... *verification of the authenticity of a digital signature in the absence of a digital certificate ... verifying that a purported owner of a public key in fact has present custody of the corresponding private key at the time a digital signature is executed ...* ")

Regarding claim 2 (Canceled)

Regarding claim 4 (Original), Haber does not teach a session key in generating digital signatures of encrypted files between the client and TSA (i.e. time source provider) for secure transactions. However, Berson disclose the generation and usage of a session key generating digital signatures in the encryption of files and enhanced securing of a transaction. (see Berson col. 4, lines 29-34: session cryptographic key generated)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Haber to generate a session key utilized in data encryption/decryption techniques as taught by Berson. One of ordinary skill in the art would be motivated to employ Berson in order to optimize and enhance procedures in the generation and authentication of digital signatures. (see **Berson** col. 2, line 12-13)

Regarding claim 5 (Original), Haber does not disclose the application of multiple nor differing errorcorrecting codes. However, Berson discloses the utilization of a session key for cryptographic techniques, and multiple or differing error correcting codes with

source calibration data. (see Berson col. 8, line 59 - col. 9, line 7: error correcting codes for transmission errors) to generate variable values.

It would have been obvious to one of ordinary skill in the art at the time the invention to modify Haber's to add the session key data transmission with some kind of error detection and correction bits by adapting the error correction codes taught in Berson. One would have been motivated to apply representation of time and error correction codes for correcting differential errors in the detected value in order to prevent a garbled key in data transmission and to produce a precise measure of the key values and ensure the integrity of documentation with an electronic time stamp. (see Berson col. 2, line 12-13)

Regarding claim 6 (Previously Presented), Haber does not specifically disclose the client producing said archived files, file attributes and time map; TSA (i.e. time source provider) retrieving time map and session key; regenerating time map; encrypting said time map with said session key and compare them. However, Romney discloses a method as in claim 4, further comprising the steps of:

a) client producing said archived files, file attributes and time map; (see Romney col. 7, lines 1-6: any collection of digital data, authenticator identification envelope consists of file specific information)

b) Time Source Provider retrieving said time map and session key; (see Romney col. 7, lines 30-36: transmit time map)

c) the Time Source Provider regenerating said time map; (see Romney col. 8, line 64 - col. 9, line 4)

d) the Time Source Provider encrypting said time map with said session key; (see Romney col. 11, line 26-28 authenticator identification envelope (i.e. time map))

e) comparing said regenerated time map to said time map. (see Romney col. 5, lines 19-25: utilize standard comparison techniques to verify a digital signature)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Haber to establish the authenticity of an electronic document utilizing digital signatures as taught in Romney. One of ordinary skill in the art would be motivated to employ Romney in order to enhance and optimize the effectiveness of security in encryption key generation and processing. (see Romney col. 4, lines 32-37)

5. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Haber-Romney-Berson as applied to claim 1 above, and further in view of Lirov et al. (U.S. Patent No. 6,785,810).

Regarding claim 3 (Original), Haber discloses wherein to utilize the generation of digital signatures and providing said signatures. (see Haber col. 2, line 66 col. 3, line 5) Haber does not disclose multiple (i.e. double) encryption for data files. However, Lirov discloses wherein the client provides multiple encryption of files. (see Lirov col. 3, lines 44-46: multiple (i.e. double) encryption for data files)

It would have been obvious to one of ordinary skill in the art at the time of the

invention to modify Haber's timestamp signature process to incorporate a procedure for the multiple encryption of files in the generation of digital signatures (see Lirov col. 3, line 44-46) of the encrypted files with encryption keys as taught in Lirov. One would have been motivated to generate encrypt signature keys for preserving the security to employ Lirov in order to provide optimum security and privacy protections without impeding performance. (see Lirov col. 2, line 29-33: *"... system and method that combines security and privacy protection without impeding data processing performance ... in a relational database ... "*).

6. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Haber-Romney-Berson as applied to claim 1 above, and further in view of Doyle (U.S. Patent No. 6, 381,696).

Regarding claim 7 (Previously Presented), a method as in claim 1, further comprising the steps of:

a) Haber does not disclose clear channel transaction. However, Doyle discloses establishing a clear channel transaction interval and pattern; (see Doyle col. 7, lines 42-45: secure SSL (i.e. clear channel) transactions)

b) Haber does not disclose the client generating clinet public/private key pairs. However, Romney discloses a client generating and encrypting data utilizing public/private key pairs; (see Romney col. 2, lines 4-50; col. 7, lines 42-45: public/private key pair) Neither Haber nor Romney discloses clear channel

transactions. However, Doyle discloses utilizing clear (i.e. secure) channel transactions. (see Doyle col. 7, lines 42-45: secure SSL (i.e. clear channel) transactions)

c) Haber discloses transactions between a client and a TSA (i.e. time source provider). (see Haber col. 2, line 66 - col. 3, 1: TSA (i.e. time source provider)) Neither Haber nor Romney discloses clear channel transactions. However, Doyle discloses utilizing clear (i.e. secure) channel transactions. (see Doyle col. 7, lines 42-45: secure SSL (i.e. clear channel) transactions)

d) Doyle discloses triggering an alarm if said clear channel transaction is not received by the Time Source Provider. (see Doyle col. 7, lines 42-45: secure SSL (i.e. clear channel) transactions (an alarm, indication of an error condition is a standard processing procedure during transaction))

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Haber to utilize client public/private cryptographic key pairs as taught in Romney, and to utilized clear (I.e. secure) channel transactions as taught by Doyle. One of ordinary skill in the art would be motivated to employ Romney in order to enhance and optimize the effectiveness of security in encryption key generation and data processing transactions (see Romney col. 4, lines 32-37), and to employ Doyle in order to enhance procedures in authentication of a digital signature. (see Doyle col. 3, lines 33-37)

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H. Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 9 am - 7 pm.

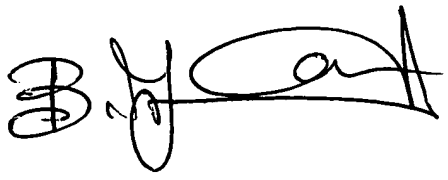
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KHS
Kyung H Shin
Patent Examiner
Art Unit 2143

KHS

May 16, 2005



BUNJOB JAROENCHONWANIT
PRIMARY EXAMINER